Abstract
This white paper describes how EMC Replication Manager integrates with Microsoft Exchange 2007 to offer an end-to-end solution of continuous availability. It discusses recommendations for configuration, mount, and restore. It also describes replication scenarios for Cluster Continuous replication (CCR), and describes step-by-step procedures for recovering Exchange 2007 databases, storage groups, and mailboxes using a recovery storage group. Finally, the paper describes how to prepare for and recover from a disaster in an Exchange 2007 environment.

December 2011
Table of Contents

Executive summary ................................................................................................................. 5
Introduction ............................................................................................................................. 5
Audience ................................................................................................................................. 6
Replication Manager architecture ............................................................................................. 6
Replication Manager GUI console and CLI ............................................................................ 7
Replication Manager Server ................................................................................................. 7
Replication Manager agents ................................................................................................. 7
Replication Manager Exchange 2007 agent .......................................................................... 8
Storage services and technologies .......................................................................................... 8
CLARiiON replication ............................................................................................................. 8
Symmetrix replication .......................................................................................................... 9
Celerra replication ................................................................................................................ 9
RecoverPoint family ............................................................................................................. 9
Microsoft VSS framework integration .................................................................................... 10
Configuring the Exchange production server ....................................................................... 12
Disable circular logging ........................................................................................................ 13
Other recommendations ........................................................................................................ 14
Configuring the Exchange backup server ............................................................................. 14
Configuring parallel consistency checking ............................................................................. 14
Protecting high-availability environments ............................................................................. 14
Cluster Continuous Replication environments .................................................................... 15
Exchange CCR storage group requirements ......................................................................... 15
Exchange CCR replication techniques .................................................................................. 16
Role-based replication ......................................................................................................... 16
Node-based replication ......................................................................................................... 21
Configuring replicas for both nodes of the cluster regardless of role .................................. 22
Standby Continuous Replication ............................................................................................ 23
Some SCR basics .................................................................................................................. 24
Replication Manager and SCR ............................................................................................ 24
Log replay and truncation ..................................................................................................... 25
Restoring with SCR enabled ................................................................................................. 26
Recovering Exchange 2007 environments .......................................................................... 26
Recovering databases ......................................................................................................... 26
Recovering a storage group ................................................................................................. 27
Recovering a database up to the failure point ....................................................................... 27
Using a differential replica to recover a database ............................................................... 28
Executive summary

Microsoft Exchange Server 2007 is the next generation of the market-leading Microsoft Exchange product line, delivering even more high-value messaging features to a wide range of customers from large enterprises down to small businesses through a highly scalable product that can help companies meet their messaging goals including:

- Enhanced security and threat protection from new techniques aimed at spam and virus elimination
- Enhanced performance utilizing a x64 (64-bit) architecture
- Additional compliance measures with expanded records management and journaling capabilities
- Simplified management by modularizing Exchange components and providing a new graphical management tool
- Increased availability techniques

Microsoft Exchange Server 2007 offers these features to help enterprises cope with the continued expansion of business-critical messaging data that they are required to manage and protect each day. Email has become the primary means of business communication and as such it is a mission-critical resource that must be protected.

EMC® Replication Manager helps customers safeguard their business-critical applications, such as Microsoft Exchange Server 2007, using either point-in-time disk-based replicas or continuous data protection sets that can be restored to any significant point in time that falls within the protection window.

At the same time, Replication Manager has deep application integration with Microsoft Exchange Server 2007. Replicas are created by coordinating with the Microsoft Volume Shadow Copy Service (VSS) to ensure a complete copy of Exchange databases (even active databases) without disrupting the production Exchange environment.

Introduction

This white paper provides additional detail concerning Replication Manager’s application integration with Microsoft Exchange Server 2007. Specifically, the paper offers the following sections:

- Replication Manager architecture overview
- Storage services and technologies
- VSS framework integration
- Configuring an Exchange production server
- Configuring an Exchange backup server
- Configuring parallel consistency checking
- Protecting high-availability environments
- Standby Continuous Replication Recovering
- Exchange 2007 environments with Replication Manager
- Exchange 2007 disaster recovery procedures

**Audience**

This paper has been written for the following audiences:

- Microsoft Exchange Server 2007 administrators responsible for implementing Replication Manager into a Microsoft Exchange Server 2007 environment
- Existing Replication Manager customers using RM to protect earlier versions of Exchange and considering migrating to Microsoft Exchange Server 2007
- EMC internal and field personnel who assist customers with Replication Manager implementations in Microsoft Exchange environments

**Replication Manager architecture**

Replication Manager uses a LAN and SAN to communicate and control storage-based functions.

Figure 1 shows the Replication Manager architecture and the components that reside in various parts of the system. An introduction to each component is provided.

![Replication Manager software architecture](image)

*Figure 1. Replication Manager software architecture*
Replication Manager GUI console and CLI
The Replication Manager Console is a portable Java application that lets you control Replication Manager from a Windows system that has a TCP/IP connection to the Replication Manager Server.

A command line interface is also provided. It can be run interactively or in batch mode.

Replication Manager Server
The server software is installed on a Windows system. It controls replication activities and stores data about each replica. The server software has three distinct components:

- **Replication Manager Server Service**, also known as the IRD, controls and coordinates replication and recovery activity for all storage corresponding to registered clients and their application sets. The IRD also handles all requests from the Replication Manager Console.

- **Policy Engine** links Replication Manager with the supported storage technologies. The policy engine is a set of dynamic libraries that link to the Replication Manager Server Service. The policy engine analyzes the storage environment and selects the appropriate storage for the replica.

- **Replication Manager Repository** is an embedded database that stores data about application sets (for instance, information about Exchange storage groups), jobs (mount, backup, log truncation, and so on), and replicas.

When installed on Microsoft Cluster Server, Replication Manager Server components fail over in the event of a cluster failover.

Replication Manager agents
Replication Manager agent software is installed on each host that participates in the replication process, including hosts that manage production data and hosts that are used to mount and back up replicas. The agent software has three distinct components:

- **Replication Manager Client Service (IRCCD)** waits for incoming requests from the Replication Manager Server (IRD), and then coordinates all operations on the agent.

- **Storage services** component manages the storage relationships between the IRCCD and the storage technologies used to create the replicas.

- **Application agents** are provided for each supported information interface, including Microsoft Exchange. Each agent is a separate library, dynamically linked and loaded with the IRCCD at runtime. The following section describes the Exchange 2007 agent in detail.
**Replication Manager Exchange 2007 agent**

To support Exchange Server 2007 on Windows Server 2003 and 2008 (x64), Replication Manager uses Microsoft VSS technology. As with agents for other applications, the Exchange 2007 agent provides Replication Manager with a logical view of the data that resides on the storage array. The agent enables Replication Manager to:

- Specify which storage groups to replicate
- Ensure that the data can be replicated safely
- Return the database to normal operation
- Dismount mailbox stores during restore operations

When replicating storage groups for Exchange Server 2007, the agent communicates with the Microsoft Exchange Information Store service and the Exchange VSS Writer to discover storage group information and create an application-consistent replica using VSS.

**Storage services and technologies**

This section summarizes the storage technologies supported by Replication Manager and how they relate to Exchange replication.

**CLARiiON replication**

On CLARiiON® arrays, Replication Manager can take advantage of both clone and snapshot functionality. Clones are fractured from the source and therefore have no impact on production environments, and are ideal for creating copies of production data for business continuity, backup acceleration, and repurposing. Snapshots offer an alternative to clones in that they require less space, but because they are pointer-based they may cause spindle contention, in which case users may opt for the performance benefit provided by clones. Since both features are included with SnapView™, customers can evaluate which makes the most sense for their particular environment. CLARiiON-based storage technologies to consider for Exchange replication are:

- **CLARiiON SnapView clone**, which creates exact copies of active production data on separate drives.
- **CLARiiON SnapView clone (remote)**, which creates clone LUNs of a MirrorView™/S secondary device (Targets that use multiple secondaries are not supported by Replication Manager.)
- **CLARiiON SnapView snapshot**, which creates SnapView snapshots of CLARiiON LUNs.
- CLARiiON SnapView snapshot (remote), which creates SnapView snapshots of a MirrorView/S secondary device (Targets that use multiple secondaries are not supported by Replication Manager.)
- SAN Copy™, which is a storage system application that copies data between storage arrays (Symmetrix®-to-CLARiiON and CLARiiON-to-CLARiiON) and within a CLARiiON array

**Symmetrix replication**

On Symmetrix arrays, Replication Manager can take advantage of TimeFinder®/Mirror (BCVs), TimeFinder/Clone (STDs), or TimeFinder/Snaps (VDEVs). Symmetrix-based storage technologies to consider for Exchange replication are:

- TimeFinder/Mirror, which creates mirror images of active production volumes from a standard device onto a BCV device
- TimeFinder/Mirror (remote), which creates mirror images of active production volumes from a standard device onto BCVs for R2 devices across an SRDF link
- TimeFinder/Clone, which creates copies of active production volumes in which the source and target devices can be either STD or BCV devices
- TimeFinder/Clone (remote), which creates copies across an SRDF link from an R1 device onto a STD or BCV on a remote Symmetrix
- TimeFinder/Snap, which creates copies of active production volumes or R1 devices onto a TimeFinder/Snap (also known as a VDEV) on the local Symmetrix
- TimeFinder/Snap (remote), which creates copies of active production volumes onto TimeFinder/Snaps (VDEVs) by way of an R2 device located on a remote Symmetrix array (connected to the production volumes using SRDF/S)
- SAN Copy (Symmetrix-to-CLARiiON)

**Celerra replication**

On Celerra® iSCSI network servers, Replication Manager can take advantage of Celerra SnapSure™ for local snapshots or Celerra Replicator™ for remote snapshots. When you create a replica using either of these iSCSI Celerra snapshot technologies, Replication Manager creates a point-in-time copy of all data on the source LUN. For the initial snapshot, Replication Manager creates a full copy of the original LUN, therefore requiring the same amount of space on the file system as the LUN. Subsequent snapshots’ space usage depends on how much the data has changed since the last snapshot was taken. For copy replicas, a full copy is created each time the job runs.

**RecoverPoint family**

Replication Manager now supports EMC RecoverPoint software, enabling users to manage applications protected by RecoverPoint Continuous Data Protection (CDP), Continuous Remote Replication (CRR), and Concurrent Local and Remote (CLR).
replication technologies. Replication Manager's support for RecoverPoint provides near-instantaneous mounting of critical business data. It allows rapid recovery of the data on a volume to any point in time (crash-consistent recovery) or to a significant point in time (application-consistent recovery). Replication Manager with RecoverPoint addresses the problem of lengthy recoveries of files and databases made by traditional backup software. It allows rapid reconstruction of a volume image that may be only seconds or minutes old.

**Microsoft VSS framework integration**

Replication Manager leverages the functionality provided by Microsoft Volume Shadow Copy Service (VSS) that facilitates the creation of application integrated shadow copy backups. Specifically, Replication Manager uses VSS to perform online replication of Exchange Server 2007 storage groups. VSS is included with Windows Server 2003 and 2008.

VSS provides the framework to create point-in-time, transportable shadow copies of Exchange Server 2007 using hardware-assisted technologies. There are three components of VSS: a requestor, a writer, and a provider. A VSS requestor is typically a backup application—it initiates the creation of a shadow copy. Replication Manager is a VSS requestor. The VSS writer is the application-specific component in the shadow copy creation and restore/recovery process. The VSS writer is provided by Exchange Server 2007. The VSS provider creates and manages the shadow copy. Replication Manager uses the EMC provider that works with its storage arrays. The Volume Shadow Copy Service coordinates these functions as shown in Figure 2.

The Exchange VSS Writer allows you to create point-in-time replicas using Full, Copy, Differential, or Incremental backup modes. Both Copy and Full backup modes back up the databases, transaction logs, and system files. Only Full mode truncates the logs after a successful backup. Both Differential and Incremental backup modes back up the transaction logs and system file. Incremental mode truncates the transaction logs after a successful backup. Replication Manager supports Full, Copy, and Differential backup modes.

These shadow copies (replicas) can be mounted, recovered, and rolled forward to restore data from one or more Exchange Server 2007 storage groups. Since these shadow copies are transportable, they can be mounted to alternate hosts for consistency checking, backup, or mailbox recovery.
When Replication Manager creates a replica of an Exchange database with the assistance of Volume Shadow Copy Services (VSS), the replica is considered application-consistent. A Full or Copy replica is considered application-consistent because it is composed of a database and a set of log files that can be replayed into the database to restore it to a consistent state. Although the replica is considered application-consistent, you will notice that the database is in a dirty shutdown state. This is because the logs contain data that needs to be written to the database files. These logs will be written during the recovery phase of restore. It is normal for a replica created using VSS to be in a dirty shutdown state.

Note the sample output from the `Eseutil /mh` command, shown below:

File Type: Database  
Format ulMagic: 0x89abcdef  
Engine ulMagic: 0x89abcdef  
Format ulVersion: 0x620,12  
Engine ulVersion: 0x620,12  
Created ulVersion: 0x620,12  
dbtime: 1366200 (0x14d8b8)  
State: Dirty Shutdown  
Log Required: 15055-15063 (0x3acf-0x3ad7)  
Log Committed: 0-15064 (0x0-0x3ad8)
Configuring the Exchange production server

The EMC Replication Manager Product Guide contains detailed installation instructions and requirements for configuring the Exchange production server. For example, data that is shared in a Microsoft Cluster Service (MSCS) environment requires the mount host to be either a standalone server or part of an alternate cluster. Ensure that you have met the prerequisite software and hardware requirements as outlined in the EMC Replication Manager Release Notes and EMC Replication Manager Support Matrix on Powerlink’s E-Lab™ Interoperability Navigator. Powerlink® is EMC’s password-protected customer and partner-only extranet.

Because the storage group replication process takes place transparently to the Exchange server, there are minimal requirements on the server itself. All Exchange mailbox database, log, and system files to be backed up must be on storage supported by Replication Manager. You can use the Exchange Management Console to relocate all of the storage group files to appropriate volumes. This includes all mailbox databases and the transaction log and checkpoint files for each Exchange storage group.

It is also best to arrange the data so that volumes used for Exchange data do not share physical volumes with other data that is not associated with that storage group. This prevents potential problems when you restore data from a replica to the production Exchange server.

A storage group consists of up to five mailbox stores, transaction logs, and system files (such as the checkpoint file). There can be up to 50 storage groups or 50 databases on an Exchange 2007 server.
When preparing your Exchange environment for Replication Manager, note the following requirements:

- The transaction log files and system files cannot be on the same volume as the mailbox database file. Use the Exchange Management Console to control the location of these files. The location of the transaction log is controlled by changing the "Log files path" property on the Move Storage Group Path dialog box. The location of the system files is controlled by changing the “System files path” property on the same dialog box.

- The checkpoint file (E00.chk) for each Exchange storage group should be located on the volume that contains the logs for that storage group. The location of the checkpoint file is controlled by the "System path location" property of the storage group. Although making the system and log file paths the same is recommended, it is not required.

- Circular logging must be disabled (see the following section).

- A domain account must exist that is both a member of the local Administrators group and Exchange Server Administrator role.

- Nested mount points are not supported. For instance, a log path of L:\Logs and a mailbox database path of L:\DB_MountPoint are not supported. DB_MountPoint is a mount point on L:. You cannot include L: and mount points on L: in the same application set.

- In any clustered environment, either Single Copy Clusters (SCC) or Cluster Continuous Replication (CCR), Replication Manager uses the Clustered Mailbox Server (virtual server) name to discover information about Exchange 2007. Make sure you register the Clustered Mailbox Server as a host in Replication Manager.

**Disable circular logging**

Replication Manager requires circular logging to be disabled. Circular logging is disabled by default when you create an Exchange storage group. If you enabled circular logging, you must disable it for proper Exchange recoverability after a VSS backup.

If you change the circular logging status of a storage group, the Microsoft Exchange Information Store service must be stopped and restarted.

Circular logging alleviates storage constraints on the transaction log volume by overwriting log files that have been fully committed to the database. Without a full history of transaction logs, you cannot replay transactions against a cloned copy of the Exchange mailbox store. When circular logging is disabled, you must be more careful with log file maintenance, because transaction logs continue to build up. Replication Manager can be used to truncate transaction logs.
Other recommendations

If you want to restore at the storage-group level, Microsoft Exchange storage groups must be arranged on physical volumes so that each storage group uses separate physical volumes for the Exchange data and the logs.

If you want to restore individual mailbox databases, each database must be located on a separate physical volume.

Configuring the Exchange backup server

To mount an Exchange replica for consistency checking only, it is not necessary to install the complete Exchange server software on the backup host. For Exchange 2007, install the Exchange Management Tools 32-bit (x86) or 64-bit (x64).

Configuring parallel consistency checking

Replication Manager offers a job setting that allows Exchange consistency checks to be performed in parallel to shorten the overall time required to complete a replication and mount of an Exchange server. Each consistency check requires a Microsoft Jet instance and Microsoft limits Jet instances to a maximum of 16. Therefore, systems can accommodate parallel consistency checking as long as there are no more than 16 consistency checks running at the same time. If Replication Manager activity causes more than 16 consistency checks to occur at the same time, the following error occurs:

An attempt to validate transaction log files failed because the database engine could not be initialized. The operation failed with error code -1214 (0xfffffb42)

In an effort to prevent this error from occurring, Replication Manager sets a maximum of 16 consistency check threads per job. However, if multiple job runs overlap, this setting may prove to be too high. In that case, administrators can change the setting by changing a registry key on the Replication Manager Client. Follow these steps:

1. Access the following registry key location:
   Software\EMC\EMC ControlCenter Replication Manager\Client\x.x.x

2. Set the PARALLEL_THREAD_NUM key to the desired number of parallel threads, up to a maximum of 16.

3. Save the changes to the registry.

Protecting high-availability environments

EMC Replication Manager can be configured for use with any of the following high-availability environments:

- Exchange Single Copy Clusters (SCC)
• Exchange Cluster Continuous Replication (CCR)
• Exchange Local Continuous Replication (LCR)

Note: EMC RecoverPoint with Replication Manager is supported in stand-alone server and Single Copy Cluster (SCC) configurations; however it is not supported in Cluster Continuous Replication (CCR) configurations.

For more information on using SCC and LCR, refer to the EMC Replication Manager Product Guide. The following sections provide more detailed information on how to configure EMC Replication Manager for use with Exchange Cluster Continuous Replication.

Cluster Continuous Replication environments

Exchange CCR is a high-availability feature of Exchange 2007 that combines asynchronous log shipping and replay features of Exchange 2007 with the failover and management features provided by the Microsoft Cluster Service (MSCS).

Exchange Local Continuous Replication (LCR) is similar to Exchange CCR but it is a method to provide a highly available solution for the databases with a single server solution without the need to perform clustering.

The Exchange CCR cluster is a two-node Majority Node Set (MNS) failover cluster with a file share witness. The active node hosts the Clustered Mailbox Server that serves Exchange data from the active copy of the storage groups. The passive node hosts a hot standby or passive copy of the storage groups and Exchange CCR continuously ships the logs from the active to the passive copy and replays the logs into the database that resides in the passive copy of the storage group. Figure 3 illustrates a standard Exchange CCR environment.

Note that the storage array where the active copy resides and the storage array where the passive copy resides do not have to be the same type of storage array, but EMC recommends the use of the same type of storage array for both nodes to ensure that the performance of each node is sufficient to handle the load imposed by Microsoft Exchange Server 2007. For example, active copies may be stored on Symmetrix and passive copies stored on CLARiiON. This affects what replication technologies will be available to create replicas on each node of the cluster.

Exchange CCR storage group requirements

To replicate, mount, and restore Exchange data in CCR environments, there are a couple of storage group requirements as follows:

• In Exchange CCR environments, you can create only one database per storage group.
• Do not attempt to replicate passive and active copies of the same Exchange CCR storage group simultaneously as this will cause one of the jobs to fail.
Exchange CCR replication techniques

Replication Manager can create replicas in an Exchange CCR environment using any of the following techniques:

- **Role-based replication** - Creates a replica of either the active copy or passive copy of an Exchange CCR storage group, regardless of which physical node currently hosts that role.

- **Node-based replication** - Creates a replica based on the particular physical node where the data is hosted, regardless of whether that node is hosting an active or passive copy of the storage group.

- **Combination replication** - Creates a replica from a specific physical node, but considers whether the node is currently hosting an active copy or a passive copy of the storage group.

---

Exchange 2007 requires that you restore only to the active copy of the storage group. If the target node for a restore is not active, fail over the cluster to make that node active before you restore.

Do not use the cluster administration tool. Use the Move-ClusteredMailboxServer PowerShell cmdlets. The following sections illustrate role-based or node-based replication scenarios and describe how to configure replications for each.

**Role-based replication**

Role-based replication refers to your ability to create replicas of Exchange storage groups based on the current role (active or passive). In this scenario, Replication Manager backs up either the active or passive copy regardless of which node currently owns it. In other words, an Exchange CCR environment has an active node and a passive node (referring to the physical machines that make up the cluster). There is also an active copy of the storage groups and a passive copy of the storage groups that may be hosted on either of the nodes (see Figure 3 for an illustration).
Figure 3. Typical role assignments: Active node hosting the active copy of the storage groups

If a failover has occurred due to some failure or because the administrator has initiated a failover for some other reason the nodes change roles as shown in the figure.

Figure 4. Reversed role assignments: Passive node becomes the active node and hosts the active copy of the storage groups
Replication Manager can configure role-based replicas as follows:

1. Make sure that you have registered the following entities in the Replication Manager Console:
   - The cluster's physical nodes
   - Exchange Clustered Mailbox Server (the Exchange virtual server)

When adding Exchange CCR nodes, be sure to use the network name, not the IP address.

2. Create an application set and select the storage groups that you want to replicate from the Exchange Clustered Mailbox Server. (Replication Manager maps both physical nodes as well so that a specific physical node can be selected as the source of the job later on.)

3. Create the first of two linked jobs from the Exchange application set that you created previously. In the first job, choose the following attributes:
   - Choose one of the two physical nodes in the Source field of the Replication Options panel of the Job Wizard.
   - Set Replicate copy when in the Job Name and Settings panel to the storage group role to replicate (either Active or Passive). In the example in Figure 6 we are replicating the passive copy of the storage groups on the physical node lrmg047.
   - Always create and schedule the job for the node that normally hosts the role you are replicating first. Then create a job for the other node. For example, if you want to replicate the passive copy, create a job for the node that normally hosts the passive copy first.
Figure 6. Role-based job replicating the passive copy in the passive node of a CCR cluster

4. Create the second of the two linked jobs from the same Exchange application set and choose the following attributes:

- Choose the other physical node in the **Source** field of the **Replication Options** panel.
- Set **Replicate copy when** to the storage group role to replicate (either **Active** or **Passive**). Choose the same role you selected in step 3. Figure 7 illustrates the job options for the second linked job.
- Choose the same role here as was selected in the job for the other physical node. Then when these linked jobs run, only one replica will be created. The replica created will contain the copy of the storage group that represents the role (either **Active** or **Passive**) selected.
Figure 7. Role-based job replicating the passive copy in the second node of a CCR cluster

- Link the jobs by choosing the first job (created above) in the Start after job field of the Starting the Job panel.
Node-based replication

Alternatively, Replication Manager can configure node-based replication by following these steps:

1. Make sure that you have registered the following hosts in the Replication Manager console:
   - The cluster’s physical nodes
   - Exchange Clustered Mailbox Server

2. Create an application set and select the storage groups that you want to replicate from the Exchange Clustered Mailbox Server. (Replication Manager maps all registered physical nodes as well so that a specific physical node can be selected as the source of the job later on.)

3. Create a job from the Exchange application set that you created previously. In the job, choose the following attributes:
   - Choose the physical node to use in the Source field of the Replication Options panel.
   - Set Replicate copy when to Active or Passive. That instructs Replication Manager to create a replica of the storage group copy on that physical host regardless of the role of the storage group that it is currently hosting.
Select the remaining job attributes as desired to replicate the storage groups on the physical node you chose as the source.

**Configuring replicas for both nodes of the cluster regardless of role**

EMC does not recommend configuring replication of both nodes regardless of role. However, Replication Manager can use Online Copy and Online Full consistency methods to control when the logs get truncated. These consistency methods work as follows:

- **Online Full** — Replication Manager replicates the storage group(s), transaction logs, and checkpoint files, and then runs a consistency check to verify the consistency of the databases and logs. If the consistency check completes successfully, Replication Manager instructs Exchange to truncate the logs so that only changes that are uncommitted to the database remain.

- **Online Copy** — Replication Manager replicates the storage group(s), transaction logs, and checkpoint files in the same way as it does during a Online Full option, however, it does not truncate the logs. Online Copy replications are often intended for testing and diagnostic purposes only.

You can configure replicas to replicate both nodes of the cluster by following these steps:

1. Make sure that you have registered the following hosts in the Replication Manager console:
   - Both Exchange CCR physical nodes
   - Exchange Clustered Mailbox Server

2. Create an application set and select the storage groups that you want to replicate from the Exchange Clustered Mailbox Server. (Replication Manager maps all registered physical nodes as well so that a specific physical node can be selected as the source of the job later on.)

3. Create the *first* of two linked jobs from the Exchange application set that you created above.

   In the first job, choose the following attributes:
   - Choose one of the two physical nodes in the Source field of the Replication Options panel of the Job Wizard.
   - Set *Replicate copy when* in the Job Name and Settings panel to the storage group role to replicate (**Active** or **Passive**). That instructs Replication Manager to replicate the node regardless of the role.

4. Choose the Online - Copy consistency method for the first job to prevent Replication Manager from truncating the logs until the second job runs.

5. Create the second of the two linked jobs from the same Exchange application set and choose the following attributes:
Choose the other physical node in the Source field of the Replication Options panel.

Set Replicate copy when to the storage group role (Active or Passive). That instructs Replication Manager to replicate the node regardless of the role.

Ensure that the Online - Full consistency method is selected for this second job. Online Full truncates the logs. These options are found in the Advanced panel of the Job Wizard. You can control the order in which the jobs run by linking them.

**Note:** Restoring replicas created by the first job requires planning. Because the second job truncates logs, the first job will always be missing logs for the time between job 1 and job 2. Those logs will be truncated and remain part of the second replica created only.

### Standby Continuous Replication

Standby Continuous Replication (SCR) was introduced in Exchange 2007 SP1. Replication Manager version 5.1.1 or later works with storage groups that have SCR enabled.

SCR is the newest continuous replication feature for Exchange 2007. It is designed for scenarios that use standby recovery servers. SCR uses the same log shipping and replay technology used by local continuous replication (LCR) and cluster continuous replication (CCR). SCR extends your deployment options, allowing you to replicate a storage group to multiple local and remote sites.

![Site-resilient environments](image)

**Figure 9. Site-resilient environments**
For more information about planning and managing SCR, see Microsoft’s TechNet website: http://technet.microsoft.com/en-us/library/bb676502(EXCHG.80).aspx. Review the “Planning for Standby Continuous Replication” section, which contains important information about optimizing your network, as well as information about truncating transaction log

**Some SCR basics**

As with the other continuous replication features, SCR-enabled storage groups cannot contain more than one database. You cannot enable SCR for a storage group that contains more than one database, and you cannot add a second database to an SCR-enabled storage group. Also, as with CCR, SCR requires that the database and log file paths be the same on the source and the target.

Instead of referring to storage groups as either active or passive, SCR refers to them as sources and targets. An SCR source storage group can be on any of the following:

- A stand-alone Mailbox Server (with or without LCR enabled)
- A Clustered Mailbox Server in a single copy cluster
- A Clustered Mailbox Server in a CCR environment

A target can be:

- A stand-alone Mailbox Server without LCR enabled
- A passive node in a failover cluster where the Mailbox role is installed, but no Clustered Mailbox Server (CMS) has been installed (there can be no active CMS)

No LCR or CCR can be enabled on the target. A source server can have multiple target servers and a target server can have multiple source servers. All Exchange target and production servers must be in the same Active Directory domain. The transaction logs are shipped from the source to the target and replayed at the target.

**Replication Manager and SCR**

Replication Manager relies on the Exchange VSS Writers to back up storage groups. There is no writer that supports backing up the SCR targets. Currently, the only way to create a replica of an SCR target using Replication Manager is to:

- Create a script that suspends replication
- Create a script that resumes replication
- Create a script that runs ESEUTIL /k against the database files and transaction log prefix
- Create a file system application set that includes the database and log volumes
- Create a job using the suspend and resume replication scripts as the pre- and post-replication scripts. Include a mount step that runs the ESEUTIL commands as a post-mount script.
Log replay and truncation

SCR includes a built-in delay for log replays. The administrator can also specify an additional delay. This is useful in the event of logical corruption of an active database; the delay could be used to prevent logical corruption of an SCR target database. LCR and CCR do not have log replay delays.

You can control log replay and truncation at the SCR target by changing the following parameters on the New-StorageGroup or Enable-StorageGroupCopy PowerShell cmdlets:

- **ReplayLagTime** – specifies the minimum amount of time (in seconds) that the Microsoft Exchange Replication Service should wait before replaying log files after they have been copied to the SCR target server. The minimum value is zero seconds, but Exchange 2007 SP1 adds another restriction that requires a minimum of 50 log files to be copied before logs are replayed. So, no matter what you choose as a ReplayLagTime, Exchange will always delay replaying logs until it accumulates more than 50 log files.

- **TruncationLagTime** – specifies the amount of time that the Microsoft Exchange Replication service should wait before truncating log files after they have been copied and replayed to the SCR target. The count begins after the log has been replayed.

Truncation of the transaction logs on the SCR source server is dependent on the status of the log files at all SCR target servers. When logs arrive at the SCR target server, they are first inspected for consistency and corruption. Then, after the replay delay, they are replayed into the target database. Before the SCR source log files can be truncated, they have to be inspected by all SCR target servers. Log truncation at the SCR source does not have to wait for the logs to be replayed at the SCR targets, as it does with LCR and CCR. However, if SCR is enabled in LCR and CCR environments, log truncation still has to wait until the log file is replayed into the passive copy. Also, if one of the SCR targets is down, log truncation will not occur at the source.

The SCR target log files can be truncated once Replication Manager creates a Full replica of the SCR source storage group. If the source storage group is in a CCR environment, the Full replica can be of either active or passive copy. A background thread runs every three minutes on the SCR target server. It determines if any log files need to be truncated. A log file will be truncated if:

- The log file has been truncated on the SCR source.
- The log file generation sequence is below the log file checkpoint for the storage group.
- The log file is older than ReplayLagTime + TruncationLagTime
Restoring with SCR enabled

If you need to restore and recover a database that has SCR enabled, Replication Manager suspends all replication before restoring the data. This includes any LCR or CCR sessions, as well as replication with all SCR targets. Once the database is recovered, you can use the **Resume-StorageGroupCopy** PowerShell cmdlet to restart the replication that was suspended. If you need to restore and recover an entire storage group, including the log volume, you will need to reseed all of the replication targets. You can use the **Update-StorageGroupCopy** cmdlet to do this. SP1 includes a new parameter “-StandbyMachine” for these cmdlets, to specify the name of the SCR target computer.

Recovering Exchange 2007 environments

It is critical that Replication Manager users are able to recover their Exchange 2007 data from a Replication Manager replica. This section describes how to recover Exchange Server 2007 data from a disk replica or import data to Replication Manager from tape.

Recovering databases

Replication Manager supports restoring and recovering Exchange 2007 storage groups, individual databases, and transaction logs. Beginning with version 5.1.2, Replication Manager supports creating, mounting, and restoring replicas of the Exchange transaction log and system file volume(s). This type of replica is a Differential replica and it does not truncate logs. Restoring just the transaction log and system file volume(s) from a complete replica (Full or Copy) was also added in version 5.1.2. Having the flexibility of restoring databases from one replica and logs from another is now possible with Replication Manager.

The high-level steps that occur during restore and recovery are:

1. Replication Manager dismounts all databases in the selected storage group(s).
2. Replication Manager sets the databases for override by restore.
3. Replication Manager sends a list of components (storage groups, database, and/or log directory) to the Exchange Store Writer.
4. The Exchange Store Writer initiates its pre-restore checks.
5. Replication Manager restores the volumes on which the selected components reside and communicates with the Exchange Store Writer when the restore is complete.
6. The Exchange Store Writer creates or updates the *EnnRestore.env* file, checks for gaps in the log sequence, plays the log files back, and then deletes the *EnnRestore.env* file.
7. Replication Manager mounts the databases.
When using replicas created by Replication Manager to recover Exchange data, the most common recovery scenarios are:

- Recovering a storage group
- Recovering a database up to the failure point
- Using a Differential replica to recover a database

The recovery scenario that is right for your situation depends on the nature of the failure. Some possible scenarios are discussed below.

**Recovering a storage group**

If you lose an entire storage group, you can use a Replication Manager Full or Copy replica to recover the storage group. All of the database (.edb), transaction log, and system (.chk) files will be restored. Replication Manager overwrites the entire volume when it restores the data. If there is any data on the volumes that you want to preserve, you should copy it to another volume before beginning the restore process.

To initiate recovery at the end of the restore, select the **Recover and Mount databases** option. The storage group will be recovered to the point in time that the replica was created. Normally, the most recent replica is used to limit data loss. You can use an older replica or even import a copy of a replica from long-term storage such as tape. Import is discussed in the *EMC Replication Manager Product Guide*.

If you do not initiate recovery, you have the opportunity to add or delete log files before you manually initiate recovery. Manipulating log files should be done cautiously by someone that is familiar with Exchange. If you manipulate the log files, you should verify that the log file sequence has no gaps before starting recovery. Run ESEUTIL /ml enn, where enn is the transaction log prefix. You initiate recovery by using the Exchange Management Console to mount the databases in the storage group. If you run into errors during recovery, you may need to delete the checkpoint file (enn.chk) or rename the log file with the highest sequence number to enn.log. When recovery is complete, delete the EnnRecover.env file from the log directory.

**Recovering a database up to the failure point**

If a database becomes corrupt, you can use Replication Manager to restore a database from a Full or Copy replica. Only the volume that the database resides on is restored. The log volume is not overwritten, so the newer logs are available for replay and data loss is minimized. In this scenario, you must restore the most recent replica otherwise there will be gaps in the log sequence.

To initiate recovery at the end of the restore, select the **Recover and Mount databases** option. Exchange will delete the checkpoint file and replay the logs in the log directory. If you do not use Replication Manager to initiate the recovery, you will need to:

- Delete the checkpoint file (Enn.chk)
Use the Exchange Management Console to mount the databases in the storage group.

Delete the EnnRecover.env file in the transaction log directory.

**Using a differential replica to recover a database**

Another Replication Manager recovery option for a corrupted or lost storage group is restoring the databases from a Full or Copy replica and the transaction logs from a Differential replica. If the logs that are currently on the disk are bad, you can use the most recent Full or Copy replica and restore the databases. Then restore the logs from the most recent Differential replica. When you restore the databases, you need to clear the **Recover and Mount databases** option. Clearing this option allows Replication Manager to inform Exchange that additional log files will be restored in a subsequent restore. When you restore the transaction logs from the Differential replica, make sure the **Recover and Mount databases** option is selected so Exchange will replay the transaction logs.

**Special considerations for some storage technologies**

When restoring a RecoverPoint replica, the entire replica is always restored. Because of this, the option to just restore the log volume from a complete replica is not supported. Support for Differential replicas was not added for two reasons. You cannot restore just a database from a complete RecoverPoint replica and RecoverPoint provides continuous replication that minimizes the need for a Differential replica. You can recover from any point in time.

A restore of a Celerra local snap is destructive. This means any newer snaps of the same source volumes are automatically deleted. Replication Manager will detect this and mark these replicas as either partially restorable or not restorable. If you restore just the databases from a Full replica, any newer replicas will be marked as partially restorable. The Differential replica is still restorable. If you restore all of the storage groups in a Full replica, any newer replicas will be marked as not restorable. To restore from a Differential replica, remember to restore just the database from the previous Full replica. Otherwise the Differential replica will not be restorable.
With the recovery storage group feature in Exchange 2007, you can mount a second copy of an Exchange mailbox database on the same server as the original database (as long as the original database is not hosted on a cluster) or on any other server that is running Exchange 2007. This action can be performed while the original database is still running and serving clients. With this capability, you can easily recover data from a replica of the database without disturbing user access to current data.

If you prefer to use third-party products such as OnTrack PowerControls instead of recovery storage groups, you can still use Replication Manager. Just mount the Replication Manager replica in read-write mode.

Create a recovery storage group from a replica

To create a recovery storage group, run the following Exchange Management Shell command:

```
new-storagegroup -server <ExchangeServerHostname> -logfolderpath "<LogPath>" -name <RecoverySGName> -SystemFolderPath "<SystemFilePath>" -recovery
```
<ExchangeServerHostname> is the name of the Mailbox Server where the recovery storage group is being created.

<LogPath> is the full path to the log file location for the recovery storage group. Use the path where Replication Manager mounts the log volume. If the production logs are in L:\Logs and Replication Manager is mounting the replica to C:\RSG, use C:\RSG\LDrive\Logs.

<RecoverySGName> is the name of the recovery storage group.

<SystemFilePath> is the name of system file path. Use the path where Replication Manager mounts the system file volume.

Figure 11. Creating a recovery storage group

The recovery storage group is created and now you need to add the databases you want to recover.

Mount and recover the recovery storage group

After creating the recovery storage group from the replica, you can mount and recover that recovery storage group in order to access the mailbox data. To do this, perform these steps:

1. Add the database to be restored to the recovery storage group by running the following Exchange Management shell command:

   ```
   new-mailboxdatabase -mailboxdatabasetorecover
   <ProductionServerName\mailboxDBtoRecover> -storagegroup
   <ExchangeServerHostname>\<RecoverySGName> -EDBFilePath
   "<pathToEDBFileForDB>"
   ```

   where:
<ProductionServerName\mailboxDBtoRecover> is the name given to the mailbox database you want to add.

<ExchangeServerHostname> is the name of the server where you created the recovery storage group.

<RecoverySGName> is the name of the recovery storage group created in the previous step.

<pathToEDBFileForDB> is the path and filename of the *.edb file that you are recovering. Use the path where Replication Manager mounts the database volume, for instance, R:\RSG\MDrive\DBs\MBX1.edb.

---

**Figure 12. Add a recovery database to the recovery storage group**

2. Delete the folders that are created under the mount point as part of running the previous cmdlets. This can be done by running the following command:

---

**Figure 13. Delete any folders created under the mount point**
3. Using Replication Manager, select the replica of the Exchange Server 2007 database from which you want to recover data. Right-click the replica and select **Mount Replica**. Select the Exchange server and the mount point used when you created your recovery storage group.

If you are mounting a Celerra or RecoverPoint replica, any changes you make while the replica is mounted will be discarded when the replica is unmounted. To get the same behavior for a CLARiiON clone replica, select the **Create and mount a snap of the replica** option. This option causes the changes to be discarded when the replica is unmounted.

![Mount Wizard (test_rsg)](image.jpg)

**Figure 14. Mount options for the replica**

4. Using eseutil, perform a soft recovery of the storage group. Open a command window and run the following command. You may need to use the /i switch also if the recovery fails with a mismatched or missing database attachment error:

```
eseutil /r E<nn> /8 /d "<PathToEDBfile>" /s "<PathtoSystemFiles>" /l "<PathToLogFiles>"
```

where:
<nm> is the logfile prefix.
/8 is the page size for Exchange 2007
<PathToEDBfile> is the location of the database file. Just use the pathname; do not include the .edb filename.
<PathToSystemFiles> is the location of the system files you used when creating the recovery storage group.
<PathToLogFiles> is the location of the log files you used when creating the recovery storage group.

Figure 15. eseutil command to perform soft recovery of a database

5. Mount the recovery database into your Exchange server by running the following Exchange Management Shell command:

```bash
mount-database -identity
<ExchangeServerHostname>\<RecoverySGName>\<mailboxDBtoRecover>
```

Figure 16. Mount the recovery database
6. Confirm that the RSG database is mounted properly by running the following Exchange Management shell command:

```
get-mailboxDatabase -status | ft Name, Server, StorageGroup, Mounted, Recovery
```

![Figure 17. Get information about the recovery database in the RSG](image)

7. Recover the mailbox from the recovery storage group by running the following Exchange Management Shell command:

```
Restore-mailbox -identity <MailboxIdParameter> -RSGDatabase <ExchangeServerHostname>\<RecoverySGName>\<mailboxDBtoRecover>
```

![Figure 18. Recover the mailbox of an existing user to an existing mailbox](image)

We recover the mailbox of an existing user, Mark Miller, to an existing mailbox. Go with the default (Yes). The mailbox will be recovered. To verify this, check that the items deleted from Mark Miller’s mailbox are recovered.
Clean up the recovery storage group

Once you have restored the mailbox successfully using the previous steps, you must clean up the recovery storage group using the following steps:

1. Dismount the database.

   ```bash
dismount-database <ExchangeServerHostname>\<RecoverySGName>\<mailboxDBtoRecover>
   ```

   ![Figure 19. Dismount the recovery database](image)

   Go with the default (Yes) and the database will be dismounted.

2. Remove the mailbox database.

   ```bash
   Remove-MailboxDatabase <ExchangeServerHostname>\<RecoverySGName>\<mailboxDBtoRecover>
   ```

   ![Figure 20. Remove the recovery mailbox database](image)
3. Remove the recovery storage group:

```powershell
Remove-StorageGroup <RecoverySGName>
```

![Figure 21. Remove the recovery storage group](image)

4. Unmount the replica

These steps allow you to restore Exchange 2007 mailboxes from a Replication Manager replica.

**Exchange 2007 disaster recovery procedures**

There are many types of failures that you will need to prepare for – from losing an individual’s mailbox to losing a database or losing an entire site. A recovery storage group can be used to recover an individual mailbox as documented. The *EMC Replication Manager Product Guide* documents the procedures for recovering a database from an existing replica. For information on recovering an Exchange 2007 server in the case of a site failure, refer to disaster recovery sections in the Microsoft Exchange Server 2007 documentation. To recover mailbox and public folder databases from a tape backup, refer to the “Importing a tape backup as a replica” section in the *Product Guide*.

**Conclusion**

Replication Manager offers comprehensive protection for Microsoft Exchange Server 2007 environments and can create disk replicas that can be mounted to test the database consistency, restored, and recovered.

The special procedures described in this white paper can help you develop replication strategies for Cluster Continuous Replication (CCR) environments using either role-based or node-based replication scenarios. You also learned techniques to
ensure that you can recover your Exchange data that has been stored in CCR environments.

Other sections describe strategies for recovery of Exchange storage groups and databases from Full and Differential replicas. This section also describes the additional steps necessary to recover data from a recovery storage group.

Finally, the section “Exchange 2007 disaster recovery procedures” provides references to material that can help RM users prepare for and recover from a disaster that destroys the data center where an Exchange 2007 production environment has been stored.

References
For more information about Replication Manager, refer to the following sources:

• EMC Replication Manager Version 5.0 Technology — A Detailed Review (white paper)
• EMC Celerra NS40 (850 User) Storage Solution for Microsoft Exchange Server 2007
• EMC Celerra NS40 (1100 User) Storage Solution for Microsoft Exchange Server 2007
• EMC Celerra NS40 (1350 User) Storage Solution for Microsoft Exchange Server 2007
• EMC Solutions for Microsoft Exchange 2007 EMC Celerra Unified Storage Platforms — Best Practices Planning (white paper)
• EMC Solutions for Microsoft Exchange 2007 CLARiiON CX3 Series iSCSI — Best Practices Planning (white paper)
• Improving Microsoft Exchange Server Recovery with EMC RecoverPoint — Applied Technology (white paper)
• EMC Replication Manager Administrator’s Guide
• EMC Replication Manager Product Guide
• EMC Replication Manager Release Notes
• EMC Replication Manager Support Matrix on Powerlink’s E-Lab Interoperability Navigator

For more information about Microsoft Exchange Server 2007, refer to the following source:

• Microsoft TechNet: Exchange Server TechCenter (This website was referenced for the definitions of certain Microsoft Exchange Server 2007 related terms.)
• Exchange Server 2007 Partners: Back-up and Archive website